A WHITE PAPER

Federal Continuity of Operations

Part 9 of 10: Training and Management

FITSI
FEDERAL IT SECURITY INSTITUTE
HELPING SECURE THE NATION'S FEDERAL INFORMATION SYSTEMS

Topic Summary:

- The five COOP audiences: executive, governance, operational, general users, and organizational
- Guidance and suggestions from commercial, federal, DOD, and Army publications
- Summary and Recommendations for next steps

Table of Contents

Illustration Index

Table Index

1.0 Introduction

Within the federal government and the Department of Defense (DOD) there exists substantial pressure to accomplish the same mission within a reduced budget. As a result, smaller programs not meeting the standards of a “national essential function” (NEF) can find it difficult to justify the expense of implementing a Continuity of Operations (COOP) Program; however, these same smaller programs must continue to function and to provide value even in the face of local disasters. This, the ninth paper in the series COOP for a Small Army Program, helps the COOP practitioner who must manage the different stakeholders that and groups who are affected by and must support a COOP Program despite the budgetary difficulties.

This paper analyzes guidance from commercial, federal, DOD, and Army publications to provide practical suggestions for how the COOP Program can be managed and the benefits of a fully-implemented COOP Plan realized within a smaller program. This paper posits that implementing a cost-effective and pragmatic COOP Program within the myriad of organizations making up the federal government and DOD augments the overall security of the nation and correspondingly allows scarce funds to be allocated most effectively.

2.0 The Five Audiences of COOP Management

Chief among the difficulties in setting up a COOP Program is to ensure that the different management requirements for a successful COOP Program implementation can be met. These audiences can be identified as *Executive*, *Governance*, *Operational*, *“General Public,”* and *Organizational*.

2.1 Executive (Decision Makers)

This group includes the organization’s decision makers, funders, and legitimate sources of authoritative power. This group must support the COOP Program or it will not succeed. Within the Army Program use case, this group includes the Program Manager and the Deputy Program Manager (the highest audiences of authority realistically available to a COOP practitioner within a small Army Program). In a commercial organization this would include the “C”-level executives.

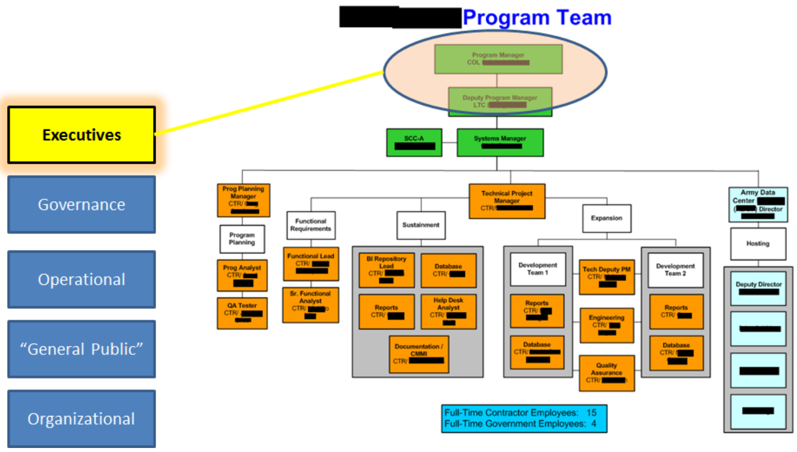
[redacted] Program Team
Program Manager COL [redacted]
Deputy Program Manager LTC [redacted]
Executives
Governance
Operational
“General Public”
Organizational
SCC-A [redacted]
Systems Manager [redacted]
Prog Planning Manager CTR/ [redacted]
Program Planning
Prog Analyst CTR/ [redacted]
QA Tester CTR/ [redacted]
Functional Requirements
Functional Lead CTR/ [redacted]
Sr. Functional Analyst CTR/ [redacted]
Sustainment
BI Repository Lead CTR/ [redacted]
Database CTR/ [redacted]
Reports CTR/ [redacted]
Help Desk Analyst CTR/ [redacted]
Documentation / CMMI CTR/ [redacted]
Technical Project Manager CTR/ [redacted]
Expansion
Development Team 1
Reports CTR/ [redacted]
Database CTR/ [redacted]
Tech Deputy PM CTR/ [redacted]
Engineering CTR/ [redacted]
Quality Assurance CTR/ [redacted]
Development Team 2
Reports CTR/ [redacted]
Database CTR/ [redacted]
Army Data Center [redacted] ([redacted]) Director [redacted]
Hosting
Deputy Director [redacted]
[redacted]
[redacted]
[redacted]
Full-Time Contractor Employees: 15
Full-Time Government Employees: 4

Figure 1: COOP Audience: Executives[1]

[1] This and the next four figures adapted by the author from a redacted Army Program management structure.

2.2 Governance (Guidance Providers)

“Governance” here refers to the organization’s ability to ensure that good COOP decisions are made. Changes to the COOP Plan, for example, would require approval from a governance board such as a Change Control Board (CCB). In the literature, a COOP governance board is typically called a Steering Committee (ICOR, p 46). This committee is made up of at least one senior leader (the Sponsor) and knowledgeable senior resources from around the organization. These senior resources give weight and substance to COOP decisions.

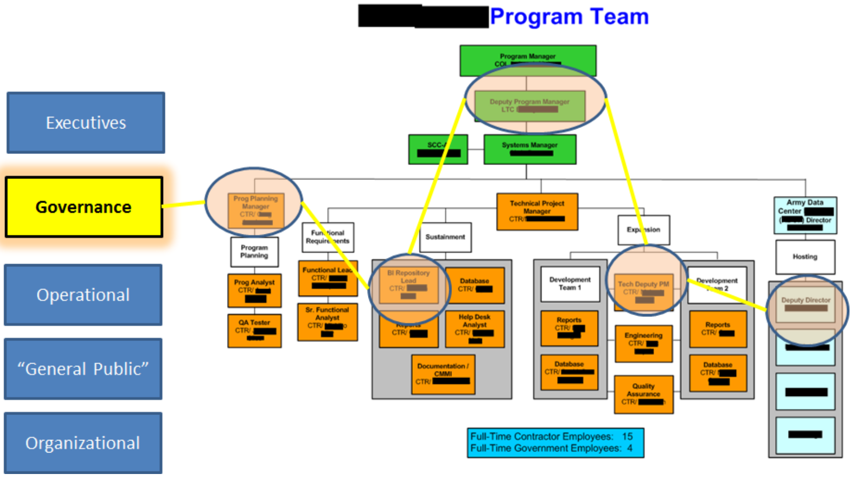
Executives
Governance
Operational
“General Public”
Organizational
[redacted] Program Team
Program Manager COL [redacted]
Deputy Program Manager LTC [redacted]
SCC-A [redacted]
Systems Manager [redacted]
Prog Planning Manager CTR/ [redacted]
Program Planning
Prog Analyst CTR/ [redacted]
QA Tester CTR/ [redacted]
Functional Requirements
Functional Lead CTR/ [redacted]
Sr. Functional Analyst CTR/ [redacted]
Technical Project Manager CTR/ [redacted]
Sustainment
BI Repository Lead CTR/ [redacted]
Database CTR/ [redacted]
Reports CTR/ [redacted]
Help Desk Analyst CTR/ [redacted]
Documentation / CMMI CTR/ [redacted]
Expansion
Development Team 1
Reports CTR/ [redacted]
Database CTR/ [redacted]
Tech Deputy PM CTR/ [redacted]
Engineering CTR/ [redacted]
Quality Assurance CTR/ [redacted]
Development Team 2
Reports CTR/ [redacted]
Database CTR/ [redacted]
Army Data Center [redacted] ([redacted]) Director [redacted]
Hosting
Deputy Director [redacted]
Full-Time Contractor Employees: 15
Full-Time Government Employees: 4

Figure 2: COOP Audience: Governance

2.3 Operational (Executable Resources)

The operational COOP team members include trained resources from around the organization. These are the resources that form the teams that execute during an emergency. Teams such as the Emergency Response Group (ERG), the Incident Response Team (IRT), even the Salvage & Restoration Team. These teams do not report solely to the COOP practitioner, and they are subject to change over time based on the normal course of employee onboarding and outboarding.

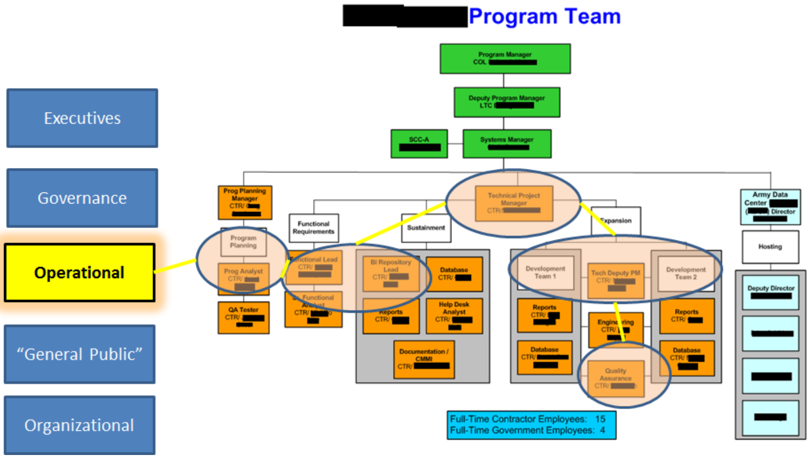
Executives
Governance
Operational
“General Public”
Organizational
[redacted] Program Team
Program Manager COL [redacted]
Deputy Program Manager LTC [redacted]
SCC-A [redacted]
Systems Manager [redacted]
Prog Planning Manager CTR/ [redacted]
Program Planning
Prog Analyst CTR/ [redacted]
QA Tester CTR/ [redacted]
Functional Requirements
Functional Lead CTR/ [redacted]
Sr. Functional Analyst CTR/ [redacted]
Technical Project Manager CTR/ [redacted]
Sustainment
BI Repository Lead CTR/ [redacted]
Database CTR/ [redacted]
Reports CTR/ [redacted]
Help Desk Analyst CTR/ [redacted]
Documentation / CMMI CTR/ [redacted]
Expansion
Development Team 1
Reports CTR/ [redacted]
Database CTR/ [redacted]
Tech Deputy PM CTR/ [redacted]
Engineering CTR/ [redacted]
Quality Assurance CTR/ [redacted]
Development Team 2
Reports CTR/ [redacted]
Database CTR/ [redacted]
Army Data Center [redacted] Director [redacted]
Hosting
Deputy Director [redacted]
Full-Time Contractor Employees: 15
Full-Time Government Employees: 4

Figure 3: COOP Audience: Operational

2.4 General Public (End Users)

The "general public" within a COOP Program includes everyone: all of the employees, the external customers, program management, even the COOP team members that are included in other groups. This serves to emphasize that a COOP Program must always reflect the audience it seeks to serve. To ensure a successful COOP program, the practitioner needs to plan and deliver the COOP message of understanding, preparation, and situational awareness that will enable the organization to survive even serious disruptions.

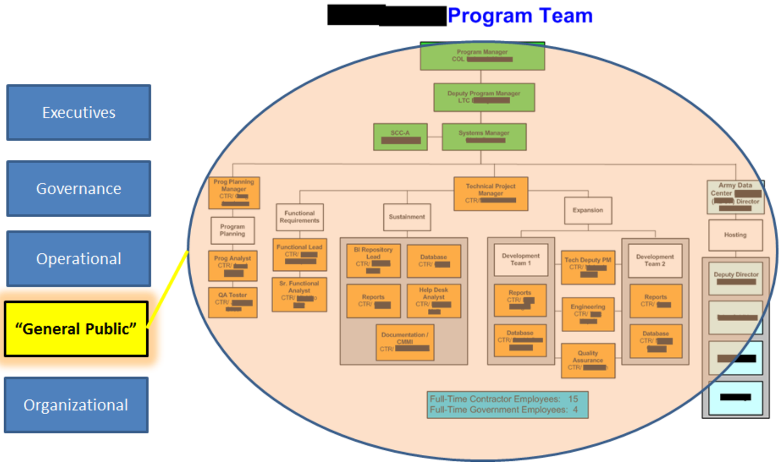

Figure 4: COOP Audience: "General Public"

2.5 Organizational (Corporate Infrastructure)

The COOP practitioner must remember to include not only the people (individuals) that the COOP Program is designed to protect but also the organizational functions such as Human Resources (HR), Accounting, Software Development, Information Technology (IT) Operations, and more. These functions must be viewed not simply from a perspective of keeping them operational during an emergency or extended disruption, but also to integrate with them as part of the ongoing COOP Program. As new software systems are deployed, for example, the COOP Plan must be updated. Additionally, if a COOP team member leaves the company, the COOP practitioner must be aware of this.

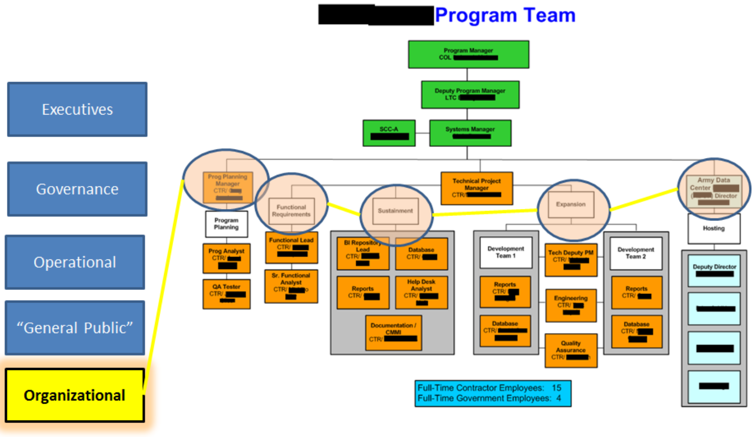

Figure 5: COOP Audience: Organizational

3.0 Management Techniques from Industry and Government

As with the other papers in this series, COOP Program management can be viewed through the prism of commercial Business Continuity Management (BCM) standards such as British Standard (BS) 25999-1:2006 ("Business Continuity Management: Part 1: Code of Practice"), federal standards such as the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-39 (“Managing Information Security Risk: Organization, Mission, and Information System View”), DOD publications like DOD’s extensions to the Project Management Body of Knowledge (PMBOK®), or the Army’s own Army Regulation (AR) 500-3 (“U.S. Army Continuity of Operations Program Policy and Planning”). This section covers each perspective and provides implementation suggestions geared toward a COOP practitioner within an Army Program, but widely applicable to any COOP practitioner within the federal sector.

3.1 Approaches from BS 25999-1:2006

BS 25999-1:2006 (henceforth referred to as “BS 25999”) provides standardized guidance for implementing a complete BCM Program. (In the federal and DOD world, the BCM Program is best represented by the COOP Program as described elsewhere in these papers.) Specific to the management aspects of a federal or DOD COOP Program, BS 25999 provides Section 5 (“BCM Programme Management”) which contains two sub-sections of special interest to the practitioner: *Assigning responsibilities*, and *Implementing continuity in the organization*.

3.1.1 Assigning Responsibilities

BS 25999 begins by acknowledging the importance of including senior management in the BCM planning process. Specifically, "The organization’s management should…appoint or nominate a person with **appropriate seniority and authority** to be accountable for BCM policy and implementation” (p 19). Practically speaking, this person is the BCM sponsor; in the DOD world getting the attention of such a high-level person, possibly at the Senior Executive Service (SES) level, may not be realistic. For the Army Program use case, an acceptable alternative is “selling the Commander,” that is, to convince the onsite high-ranking officer of the necessity for the COOP Program.

BS 25999 goes on to recommend that “top management may nominate representatives across the business by function or location to assist in the implementation of the BCM programme” (p 20); these people effectively form the Steering Committee mentioned above. The advice from BS 25999 is to build this group based on the size of the team; for the Army Program the Steering Committee includes just a handful of individuals that have deep knowledge of the Program’s mission and functions at a high level.

3.1.2 Implementing Business Continuity in the Organization

BS 25999 has general guidance here: the practitioner should define tailored activities to design, build, and implement the BCM (COOP) Program. These activities should:

- *Communicate* the plan to stakeholders; practically, this includes defining emails, “tweets,” online Web portals, posters, and so on to ensure that everyone knows about COOP. This especially concerns the “general public” COOP audience defined above.
- *Arrange* for appropriate training. This transcends any particular COOP audience: executives approve funding for training; governance validates the need for training; team members learn their responsibilities from training; the “general public” is made aware of COOP processes and procedures during training; and, organizational structures integrate training requirements (such as automatic basic COOP awareness during new employee onboarding.
- *Exercise* the continuity capability. As with training, COOP exercise plans ensure that all targeted individuals get an opportunity to practice their skills and gain in confidence.

3.2 Approaches from NIST

This series of papers has emphasized how NIST publications align to the DOD and the Army. Although created to provide guidance and standards for the federal government, NIST documents have wide applicability throughout the private and public sectors. For this paper, management aspects from NIST's SP 800-39 are reviewed. NIST's specialty in Information Security (INFOSEC) applies critically to business continuity and COOP.

Within SP 800-39, NIST identifies three tiers for establishing a risk management program that help in managing a successful COOP Program: organization level, mission/business process level, and information system level and provides the following graphic:

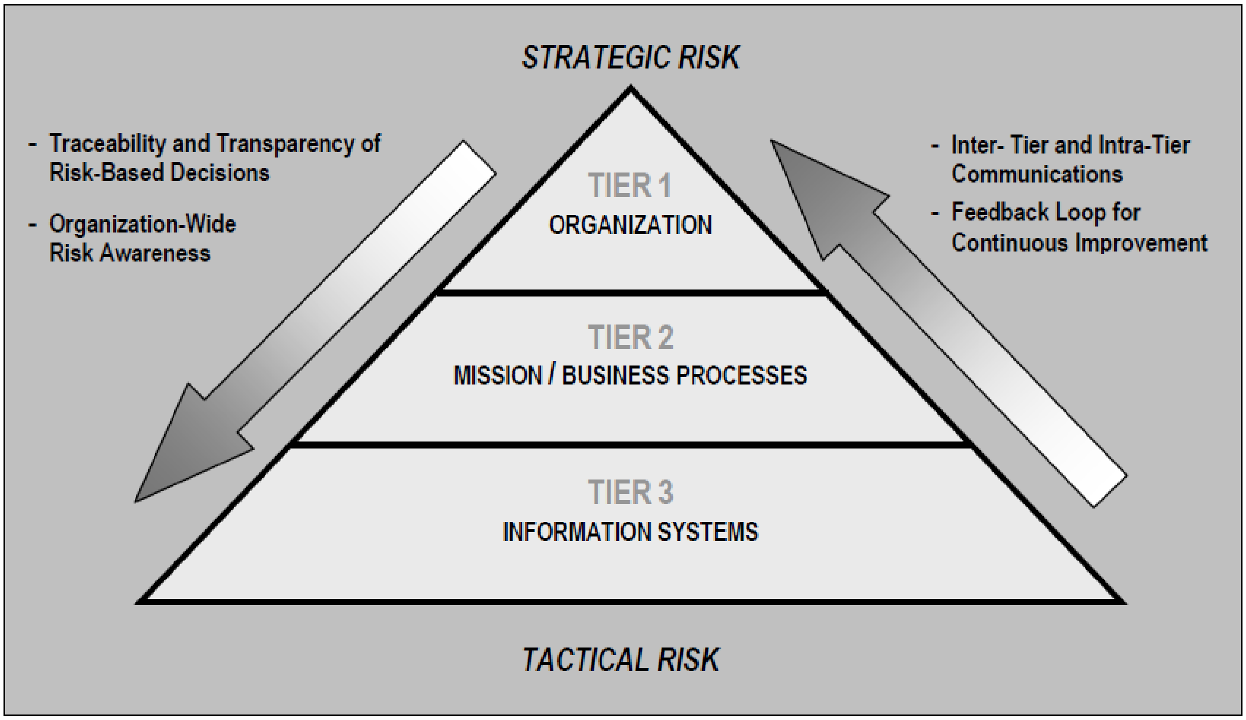
STRATEGIC RISK
- Traceability and Transparency of Risk-Based Decisions
- Organization-Wide Risk Awareness
TIER 1
ORGANIZATION
TIER 2
MISSION / BUSINESS PROCESSES
TIER 3
INFORMATION SYSTEMS
- Inter- Tier and Intra-Tier Communications
- Feedback Loop for Continuous Improvement
TACTICAL RISK

Figure 2: NIST's Three Management Tiers[2]

NIST's *organizational management view* establishes and implements governance structures consistent with the strategic goals and objectives of organizations and the requirements defined by federal laws, directives, policies, regulations, standards, and missions/business functions. NIST identifies the need for a governance function that requires the COOP practitioner to define performance-based outcomes for the COOP Program exercises. From a senior management perspective, the practitioner needs to ensure that senior executives are kept informed of how the COOP program is impacting the organization's bottom line (in the Army Program, this translates to cost avoidance and the ability to redirect saved existing funding to new projects).

The mission/business process perspective works by designing, developing, and implementing mission/business processes to support the missions/business functions defined at Tier 1. Organizational mission/business processes guide and inform the development of an enterprise architecture that provides a disciplined and

[2] Source: SP800-39, p 18.

structured methodology for managing the complexity of the organization's information technology infrastructure. From a management view, this translates to the COOP practitioner using the Steering Committee and subject matter experts (SMEs) from the COOP Teams to align identified business risks with overall strategic objectives.

Based on the NIST Special Publication's (SP's) emphasis on IT and information systems, it is no surprise that the third tier includes integrating risk management into all phases of a system's lifecycle. This corresponds well to the application of management support functions to deliver COOP training and exercise plans throughout the entire organization (the "general public" audience) and the need to tie COOP Program awareness into organizational functions such as HR and accounting. (Within the Army Program use case, examples include the Program Management Office, Quality Assurance group, and Business Process Analysis group.) The goal is a holistic engagement of the entire enterprise, program, or department to understand the COOP Program's objectives and goals.

3.3 Approaches from DOD PMBOK® Extensions

In 2003, DOD released publicly-available "extensions" to the Project Management Body of Knowledge (PMBOK®) created by the Project Management Institute (PMI). These extensions tie project management best practices to DOD acquisition laws, regulations, and policies. The extensions specify three areas that are of interest to the COOP practitioner from a management perspective: 1) Maintain COOP as an ongoing program; 2) Keep in mind the contractor-driven nature of DOD acquisitions; and, 3) Ensure that the COOP Program can demonstrate its value demonstratively ("earned value management" to use the PMI and DOD phraseology).

The first COOP management guidance from DOD's PMBOK® extensions that applies specifically to the COOP Program as exactly that – a *program* that exists "as a group of projects managed in a coordinated way to obtain benefits not available from managing them individually" (p 14). From a management view, that means that the COOP Program must be broken up into subplans as directed within the other papers in this series. From a management vantage, it requires the COOP practitioner to interact with workers and COOP team members not in their direct chain of command. In such a matrixed environment, the COOP practitioner must have proper authority granted (at the executive level in the commercial world) to ensure that the direct project managers for COOP tem members can schedule time and resources for COOP support. This can be accomplished by including those direct project managers as stakeholders throughout the COOP planning and implementation process.

One management element specific to the federal and DOD worlds is the fact that it is usual for many functions to be carried out by external contractors. In fact, all functions not deemed "inherently governmental" would fall into the DOD acquisitions process. Since much of the COOP Program implementation involves work that falls into this category (for example, COOP site maintenance and IT operations support) the COOP practitioner must account for "contracting for, controlling, and evaluating the technical performance of the contractor(s)" (p 26). This enhanced level of control has management significance for the COOP planning process; contractual agreements with the contractors in question will go a long way in coloring the way in which the COOP Plan is created and implemented. Thus, the COOP practitioner within the Army Program would be wise to become familiar with the DOD acquisition lifecycle (such as the DOD 5000-series available from the online DOD web site http://www.dau.mil/pubs/pubs-main.asp).

Another management element extolled by the PMI and especially relevant within DOD is the *earned value management system* (EVMS). The DOD PMBOK® extensions describe EVMS as "us[ing] standard cost/schedule data to evaluate a program's cost performance (and provide an indicator of schedule performance) in an integrated fashion. As such, it provides a basis to determine if implemented risk-handling strategies are achieving their forecasted results" (p 160). From a management view, EVMS means that the COOP practitioner has defined measurable forecasts for expected work to be accomplished (from creating the COOP Plan to implementing ongoing Exercise and Training Programs) and for performance measurements to be possible. Within the Army Program use case, these performance measurements may include the time required for alternate servers to become available in the event of an outage as well as the number of error reports submitted in a given time period.

3.4 Approaches from AR 500-3

This series has quoted extensively from the Army's Regulation 500-3 for COOP Program Policy and Planning. Two areas that lend themselves well to discussions from a purely management view point are the explicit *roles and responsibilities* as well as the "Management Control Evaluation Checklist" provided in the Regulation.

3.4.1 Roles and Responsibilities

Every Army Regulation (and, in fact, every DOD policy statement) explicitly lays out the requirements for each role within the hierarchy. In the case of AR 500-3, the roles are defined as:

Heads of Headquarters, Department of the Army Secretariat, and Staff Agencies. These *high-level* positions (truly similar to executive level in the commercial world) are responsible for defining a strategic COOP Plan and executing on that plan. The COOP practitioner needs to ensure that COOP planning performed at the individual program level is properly informed by top-level COOP plans; the best way to do this is to approach the senior commander (the "sponsor" within the local Army Program) and request a copy of the next-level command's COOP Plan (such as Army Material Command, or perhaps the Army Sustainment Command, or some other command; it depends upon the reporting structure and hierarchy of the Army Program in question).

The Administrative Assistant to the Secretary of the Army. This position is responsible for providing specific planning guidance to the above higher-level executive group. Its mission to provide coordination of all Army COOP Programs means that it can provide *authoritative answers* to the COOP practitioner to answer specific questions. For example, to determine if a given local Army Program mission essential function (MEF) ties into a national essential function (NEF).

The Deputy Chief of Staff, G–3/5/7. This policy group is responsible, along with the G-6 that handles information management, to create the policy documents that drive Army COOP (including AR 500-3). The COOP practitioner uses this in a management context to create conformant COOP Plans and implementation programs. The practitioner can also use this group to support organizational integration; for example, to tie new employee Common Access Card registrations with the need to have initial COOP awareness training.

Commanders and/or the senior Army official responsible for the Army Command (ACOM), Army Service Component Command (ASCC), or Direct Reporting Unit (DRU), as well as *Garrison Commanders.* These are the implementing Commanders within individual Components; as such they are generally higher in the hierarchy than the individual Commander to the local Army Program use case that this series of papers have held up as an example. However, the management interface is the same: to ensure a successful COOP Program implementation, the practitioner must ensure that support is forthcoming for the program (authority and funding) and that the COOP Program as implemented directly aligns to the COOP Program for the next-higher command.

3.4.2 Management Control Evaluation Checklist

The final COOP Program management support tool from AR 500-3 includes the Management Control Evaluation Checklist from Appendix F within the Regulation. This checklist contains a number of useful questions that can help the COOP practitioner identify if a particular COOP Program has been implemented to meet requirements:

Table 1: AR 500-3 Management Checklist Items

AR 500-3 Management Checklist Item	Notes
Have effective management controls been established for Army COOP Program standards?	Ties directly to the Executive audience; within the Army, this requires integration with higher-level COOP Plans and reference to publications from G-3/5/7. Within the federal government, this would be driven by appropriate Federal Emergency Management Administration (FEMA) Federal Preparedness Circular (FPC) 65)
Is there reasonable assurance that obligations and costs associated with the Army COOP Program are in compliance with applicable laws?	Best thought of from the Governance audience; this question is answered if the COOP practitioner has applied contractual guidance and oversight as directed by DOD's 5000-series of acquisition publications and the DOD PMBOK® extensions.
Is there reasonable assurance that the Army COOP Program and its associated funding are safeguarded against waste, loss, unauthorized use or misappropriation?	Similar to the above, the Governance audience provides the assurance that contracts issued to support a COOP Program have met stated requirements. This is a difficult section to handle because the COOP Plan must be able to improve continuously. This emphasis on improvement (that is, *change*) may require for COOP contracts to be written extremely carefully.
Is there reasonable assurance that the appropriate funding sources are utilized for and targeted against specific efforts associated with the Army COOP Program?	Integrates the Operational audience to ensure that the "specific efforts" within the Army COOP Program have been considered as individual mitigation controls were identified and implemented as part of the COOP Program implementation. Also integrates the Governance audience to analyze COOP Program change requests carefully to ensure that such changes do indeed map directly to Army COOP requirements.
Is there reasonable assurance that the Army infrastructure, both physical and cyber as identified in the Army COOP Program, is available and functional under all hazardous or potentially hazardous	The NIST SP 800-34 ("Continuity Planning for Federal Information Systems") as well as Department of the Army (DA) Pamphlet (Pam) 25-1-2 ("Information Technology Contingency Planning") both provide guidance on how to protect the IT infrastructure as part of an implemented COOP Program. From a management perspective, this control also implies that the Operational COOP team is trained and aware of COOP requirements; thus, an Exercise Plan has been created and is actively in process.

AR 500-3 Management Checklist Item	Notes
conditions both natural and man-caused?	
Is there reasonable assurance that Army COOP Responsibilities are being fulfilled?	Ties into continuous improvement via Exercise and Training Plans. Integrates both the "General Public" audience (users, customers, other external stakeholders) and can help any program to provide a competitive edge based on its demonstrated ability to continue operations despite serious business disruptions.

4.0 Concluding Remarks

4.1 Summary

The COOP practitioner has a difficult job to Initiate and maintain a COOP Program in the federal space, and this job is made even more difficult in the context of a smaller program that does not meet the criteria as either a "national essential function" (NEF) or as supporting such a function. To establish a COOP Program in this scenario requires creativity and the need to manage five different audiences of stakeholders: the executive decision makers, the governance guidance providers, the operational executable teams, the general users, and the organizational infrastructure.

This paper has analyzed guidance from the commercial, federal, DOD, and Army sectors to provide practical advice to the COOP practitioner so that these smaller programs can provide the confidentiality, integrity, availability, and information currency that all government customers deserve. Moreover, applying defense-in-depth COOP Programs to these programs and operations "in the small" combine to provide a significant continuity capability for the nation at a minimal cost.

4.2 Recommendations

This paper has applied a tailored management approach strategy to its Army Program use case and has provided a number of recommendations as shown in the table below:

Table 2: Recommendations

Recommendation	Rationale
Adapt management plans to audience levels	This paper identified five audience levels: Executive, Governance, Operational, General Public, and Organizational. Each audience has its own needs and responsibilities. Integrating with the entire organizational infrastructure (such as onboarding / outboarding) is perhaps the most critical aspect of an implemented COOP Program.
Obtain formal authorization	It is not enough to have the expressed support of senior management in a COOP Program; one must also have this expressed *formally* (written). The problem is that, for any COOP Program, the team members will not report directly to the COOP

Recommendation	Rationale
	practitioner. Integration with existing project leads and managers must be considered, as well as the fact that such project leads will most likely not be too pleased to "share" key resources with the COOP practitioner.
Organizational integration means communication and training	Employees throughout the organization must be "sold" on COOP as on any other business idea. COOP Plans in particular depend on the dedication of key employee resources, but also depend on the entire workforce having a modicum of preparedness and training prior to an emergency incident.
Make the COOP Program results quantitative	Both NIST and DOD stress the importance of creating meaningful and realistic performance goals for the COOP Program and then measuring the results from exercises and training. Results can be expressed as user feedback, or as monitored statistics (such as number of reported user outages), or as compliance (number of employees who have taken a COOP training test). In DOD especially this means expressing return using earned value measurements.
Apply best-practices checklists	AR 500-3 has its own management checklist highlighted within this paper, but all authoritative federal, DOD, and Army COOP publications have similar checklists. These checklists help the COOP practitioner to ensure that COOP Programs are tailored and aligned to meet organizational goals in a cost-effective and best-value method.

4.3 Next Steps

The nine papers thus far presented in this series on Continuity of Operations (COOP) have provided a working blueprint for a COOP practitioner to implement a functional and effective COOP Program, especially within the context of a small Army Program. This leads to the tenth and final paper in the series: a sample COOP Plan based upon sound federal, DOD, and Army policy and applicable as a starting point to a wide variety of programs and organizations within the federal sector.

Appendix A: Acronyms and Abbreviations

AR	U.S. Army Regulation
BCM	Business Continuity Management
BS	British Standard
CCB	Change Control Board
CIO	Chief Information Officer
COOP	Continuity of Operations
DA	Department of the Army
DOD	Department of Defense
DR	Disaster Recovery
EVMS	Earned Value Management System
ERG	Emergency Response Group
FEMA	Federal Emergency Management Administration
FPC	Federal Preparedness Circular
G-3/5/7	Responsible for policy and planning development for the Department of the Army.
G-6	Responsible for the information management function for the Department of the Army.
HR	Human Resources
IA	Information Assurance
ICOR	The International Consortium for Organizational Resilience
IRT	Incident Response Team
IT	Information Technology
NIST	National Institute of Standards and Technology
Pam	Pamphlet
PMBOK®	Project Management Body of Knowledge
PMI	Project Management Institute
Rev.	Revision
SES	Senior Executive Service
SME	Subject Matter Expert
U.S.	United States

About the Author

Andrew Bruce is a Cloud Architect for D&SCI in the Army Programs group out of Aberdeen Proving Ground, MD. D&SCI provides professional services to the Federal Government and the Department of Defense, specializing in customizing and developing architecture and governance models that enable tight integration to the Army's datacenter consolidation and cloud virtualization enterprise portfolio initiatives. Mr. Bruce's job responsibilities include: working directly with customers and partners for new business development, supporting proposal efforts, overseeing Army customers' network infrastructure, working with project managers to ensure project completion, managing software development efforts throughout the entire system life-cycle, and leading new technology research and proofs-of-concept. After a career spanning three decades in shrink-wrap, commercial, and corporate software development, Mr. Bruce is focusing on Information Assurance to achieve his goal of building and managing large data centers providing cloud computing utility services for commercial and Government customers. Mr. Bruce holds the CISSP, PMP, and FITSP-D certifications as well as a Master's Degree in Information Assurance from Norwich University.

Reference List

[AR500-3] DA. April 18, 2008. Army Regulation 500-3: U.S. Army Continuity of Operations Program Policy and Planning. <http://www.fas.org/irp/doddir/army/ar500-3.pdf>. Accessed: June 12, 2011. 39 p.

[BS25999] BSI. November, 2006. Business Continuity Management: Part 1: Code of Practice. London. 50 p.

[DOD-PMBOK] DOD. June, 2003. U.S. Department of Defense Extension to: A Guide to the Project Management Body of Knowledge (PMBOK® Guide). <http://www.dau.mil/pubs/gdbks/DoDExtPMBOK--June%2003.pdf>. Accessed: July 11, 2011. 288 p.

[ICOR] Business Continuity Services, Inc. 2009. Essentials of Business Continuity Management Series: The BCM Program Development (Week 2 Reading). ICOR: Lombard (IL). 66 p.

[SP800-39] NIST. March 2011. SP 800-39: Managing Information Security Risk: Organization, Mission, and Information System View. <http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf>. Accessed: July 11, 2011. 88 p.